BITCOIN: THE DECENTRALISED VIRTUAL CURRENCY AS A CRIMINAL TOOL

Dániel Eszteri,
Dr, Criminal Case Administrator, Budapest Police Headquarters' Cybercrime Unit

INTRODUCTION

In January 2009, the Japanese software designer Satoshi Nakamoto invented a virtual currency named Bitcoin and released software for managing transactions in the new money ([1]).

It consists solely of bits and bytes, but we cannot see it as a coin or banknote on the market. There is no cover in terms of gold or stocks, in fact, nothing but the source code of the software which consists of 31 000 lines of code ([2]). The payment system is completely decentralised and so contains no central organisation which monitors transactions. Many people use this new currency to pay for services or products on the Internet, since it is not less safe than traditional payment systems.

The anonym currency can be a perfect tool in the hands of criminals to reach their goals. Law enforcement authorities like the FBI have dealt with the question in a long report that recently leaked to the Internet ([3]). It can be interesting to examine the 'Bitcoin problem' from this point of view too, because the anonymous money transferring possibility seems to be the root of money laundering at first sight.

THE ESSENTIAL CHARACTERISTICS OF BITCOIN

Bitcoin is not a concrete, physically existing currency, but virtual money: an amount associated with a so-called virtual wallet. First, we have to download software from the Internet, which is also called Bitcoin. We can find this on the official homepage of the virtual currency ([4]).

This software functions as a digital wallet on our computer after installation and stores our virtual money. Our wallet is nothing but a file on our hard drive named 'wallet.dat' ([5]). Bitcoin software is open-source, available for almost every operating system, updated regularly and contains every necessary function for sending and receiving Bitcoin.

ADVANTAGES AND DANGERS OF THE LACK OF CENTRAL CONTROL

Due to the Bitcoin network feature that users give no personal information about themselves and that there is no central control authority behind the system, the identification of

([1]) Nakamoto, S., 'Bitcoin: A Peer-to-Peer Electronic Cash System', http://bitcoin.org/bitcoin.pdf (1.6.2013).

([2]) Davis, J., 'The Crypto-Currency', http://www.newyorker.com/reporting/2011/10/10/111010fa_fact_davis (2.6.2013).

([3]) Federal Bureau of Investigation (2012), 'Intelligence assessment: Bitoin virtual currency: Unique features present distinct challenges for deterring illicit activity', http://cryptome.org/2012/05/fbi-bitcoin.pdf (31.5.2013).

([4]) Bitcoin webpage, http://bitcoin.org/ (4.6.2013).

([5]) Bitcoin on Wikipedia, https://en.bitcoin.it/wiki/Wallet (4.6.2013).

suspicious transactions and users or obtaining transaction logs seems impossible at first sight. Nevertheless, the network has features which can help us track transactions and link them to someone. First, every transfer is public and can be seen on http://www.blockexplorer.com or http://blockchain.info websites ([6]). We do not have to request transaction records from authorities or financial institutions, since they can be browsed freely on the Internet. Every single transfer made by a suspected Bitcoin address can be followed along the chain.

However, it is not guaranteed that the person behind a transfer can be identified since the information includes no personal data — especially not the sender's or receiver's IP address — but merely the amount transferred between two public keys.

We have to keep in mind that most people use Bitcoin as a simple, anonymous, online payment tool and not as a currency to replace real world money. Most users buy Bitcoin for a certain purpose (for example to buy something in a web shop), but sooner or later they change back to real world currencies.

Official currencies can be changed to Bitcoin and back on some special exchange websites, such as the Japan-based MtGox (http://mtgox.com). To use services offered by the website, users have to register an account and give it an account name, password and e-mail address. This information can be a good starting point for further identification. The operators of the website could confirm whether or not someone is the user of a certain Bitcoin address registered on their website. If the answer is yes, they could provide further information, such as the registered account name, e-mail address, or IP-addresses used during logins ([7]). There are also exchange sites which ask for the bank account numbers of users, and so the service providers can transfer the amount changed in real world money. A bank account's transactions and documents concerning the owner of the account mostly provide enough information to identify a person.

According to the FBI, it is good to keep in mind that some users publish their Bitcoin addresses on online forums in their comments.

MONEY LAUNDERING WITH VIRTUAL CURRENCIES

It seems that Bitcoin could be an ideal tool to hide money made by committing a crime — money laundering — because of the anonymous paying opportunity and the absence of transaction costs. It is possible since such attempts happened recently with other virtual currencies, like a currency of an online game that is used to buy virtual items on the game's marketplace.

One good example is when an online, organised crime group changed their crime-related money to an online game's virtual currency on a special exchange website. Later they bought several virtual items (like virtual swords or armours) using the virtual world's in-game market and sold them to other players for real-world 'clean money'. Popular in-game currencies can be changed to real world money on several websites. There are also online games where the developers have made it possible to exchange virtual money for real currencies via the game clients themselves (for example 'Linden Dollars' in life-simulator 'Second Life' or 'gold' in the fantasy role-playing game 'Diablo III').

Coming back to our original topic, it is possible (criminally) to commit money laundering when someone uses Bitcoin exchange as a *modus operandi*. Someone changes criminally acquired money to Bitcoin and then forwards this to various addresses. However, it is possible to track the transactions because they are public and can be accessed by everyone on the Internet. Information could also be available in the log files of exchange websites where people can change their Bitcoin to real-world currencies.

BITCOIN THEFT

Bitcoin represents a certain value on the Internet, and we should thus keep in mind that it could be a possible target for thieves, as real-world money is.

The most important factor in these abuses is the virtual wallet file (wallet.dat) which contains the

([6]) Nakamoto, S., *supra nota* 1, p. 6.

([7]) Federal Bureau of Investigation, Intelligence Assessmen, *supra nota* 3, p. 10.

actual amount of a user's Bitcoin. If someone deletes this file — and no backup has been made — the user could lose access to the Bitcoin forever. Bitcoin will not be deleted from the system, but the user loses the public and private key pairs which are crucial for access and transactions.

A more sophisticated criminal behaviour is when somebody steals virtual money, not directly, but by trying to impact other computers to mine Bitcoin, creating a Bitcoin-miner zombie network without the permission and knowledge of the owners of participating computers. Computer networks created with such illegal intent are called botnets. At first the cybercriminal needs to install a virus on the target computer that uses its video card's or CPU's computing power to mine Bitcoin. This can be achieved most easily by spams (unsolicited bulk messages) or phishing websites.

An example of this phenomenon was the malware named *ZeUs*, which used the computer's resources to illegally mine Bitcoin. This harmful software spread through deceptive advertisements posted to various websites in the first half of 2011 ([8]).

Other sources mention that larger computer networks would be ideal for cybercriminals for joint Bitcoin-mining (e.g. a company's or a university's local network). This technique is more expedient, because effective mining typically requires excessively high calculating power ([9]).

BUYING ILLEGAL GOODS WITH BITCOIN

There are several pages on the Internet where Bitcoin can be used as a paying option. We can browse clothes, books, trinkets, or computer parts ([10]).

According to an article published on *gawker.com* on 1 June 2011, there is a webpage where we can buy any drug imaginable. The page is called *SilkRoad* and can be visited only through a special anonymous browser called *Tor (The Onion Router)*. After some search and registration effort we can look at the world's largest drug market, where we can order anything from marijuana to heroin or cocaine! However, drugs are not the only things that can be purchased: we also find tools for growing or producing drugs; we can even order ammunition, registration codes for websites, licences, etc., all of which can only be purchased with one type of currency: Bitcoin ([11]).

Sadly, virtual money can be an excellent tool for criminal activities, because it is nearly impossible to trace who sent what amount to whom.

CONCLUSION

The technology behind the virtual currency is a novelty which means a paradigm shift without parallel among financial systems, and it is still unclear what may become of it, since the tools necessary for its greater evolution are still under development.

It is presently very difficult to form an opinion of this virtual phenomenon's future since it is too new to interpret it clearly. We have to pay close attention not just to the decentralised virtual currency, Bitcoin, and its role in future crimes, but to other (centralised) types of virtual money-like currencies of online games to handle possible dangers suitably. We have to keep in mind that virtual currencies and items represent a real product in the online world and have value in physical world's money too. My essay was written to serve this goal.

([8]) Segura, J., 'Zeus, Bitcoin and the Ub3erhackers', http://blog.sparktrust.com/?p=572 (11.6.2013).
([9]) Bitcoin forum, https://bitcointalk.org/index.php?topic=11506.0 (11.6.2013).
([10]) Bitcoin wiki, https://en.bitcoin.it/wiki/Trade (13.6.2013).
([11]) Fischermann, T., 'Anarcho-Geld', http://www.zeit.de/2011/27/Internet-Bitcoins (10.6.2013).